

UNITED STATES DISTRICT COURT

UNITED STATES DISTRICT COURT
LAS CRUCES, NEW MEXICO

FEB 27 2025

for the
District of New Mexico

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)Grey Apple iPhone, Dark Grey Apple iPhone, Black
Apple iPhone and Black Motorola Cell Phone

Case No. 25-354MR

MITCHELL R. ELFERS
CLERK OF COURT

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See attachments A1, A2, A3, and A4.

located in the _____ District of _____ New Mexico _____, there is now concealed (identify the person or describe the property to be seized):

See attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

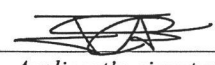
The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1349	Conspiracy to Commit Wire Fraud
18 U.S.C. § 1956(h)	Conspiracy to Launder Monetary Instruments

The application is based on these facts:
See attached affidavit.

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Juan C. Sanchez, Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ (specify reliable electronic means).

Date: February 27, 2025


Judge's signature

City and state: Las Cruces, New Mexico

Gregory B. Wormuth

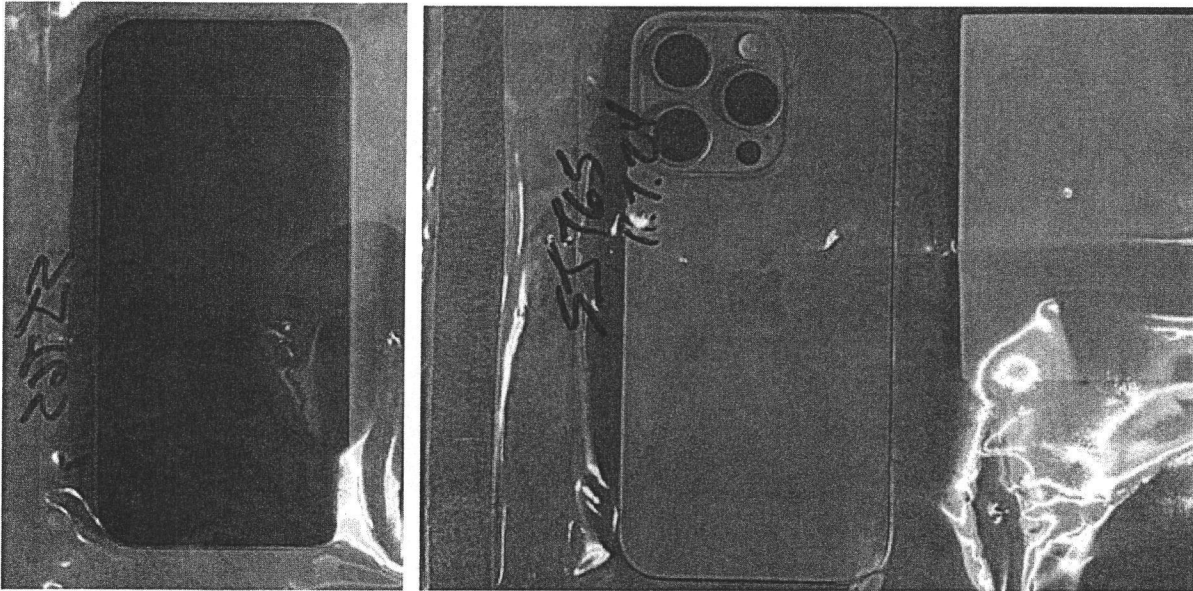
Chief U.S. Magistrate Judge

Printed name and title

ATTACHMENT A1

PROPERTY TO BE SEARCHED

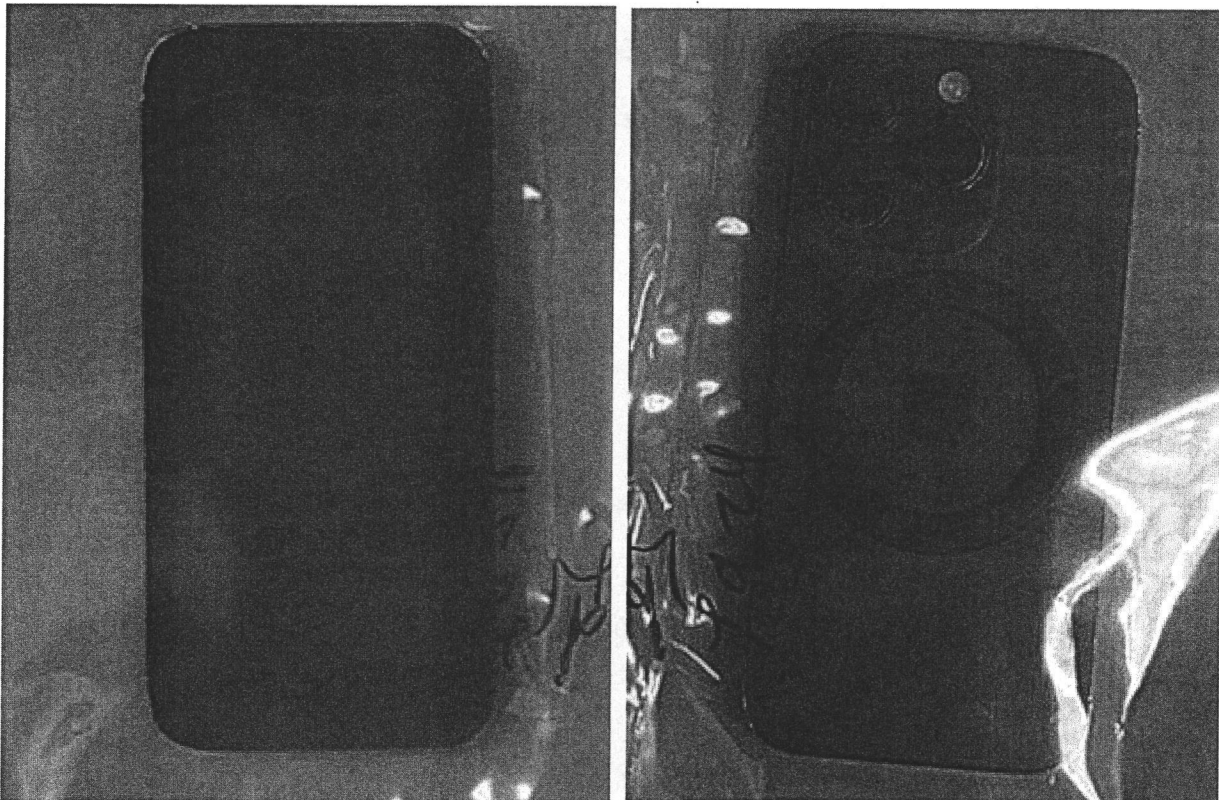
The property to be searched is a grey Apple iPhone that was initially seized by Gainesville Police Department on June 25, 2024, before being transferred to Homeland Security Investigations on January 31, 2025, as it was determined to be evidence in the criminal matter, including any Subscriber Identity Module (SIM) cards or other removable storage media contained therein. The front side of the Subject Telephone has a touch-screen display, and a camera is located near the middle of the top edge. The rear side of the Subject Telephone has four cameras in the top-left corner, and a metallic Apple logo is depicted near the middle. The Subject Telephone is currently stored at the Homeland Security Investigations office located at 1701 S. Columbus Hwy. Deming, NM 88030. The Subject Telephone is depicted below.



ATTACHMENT A2

PROPERTY TO BE SEARCHED

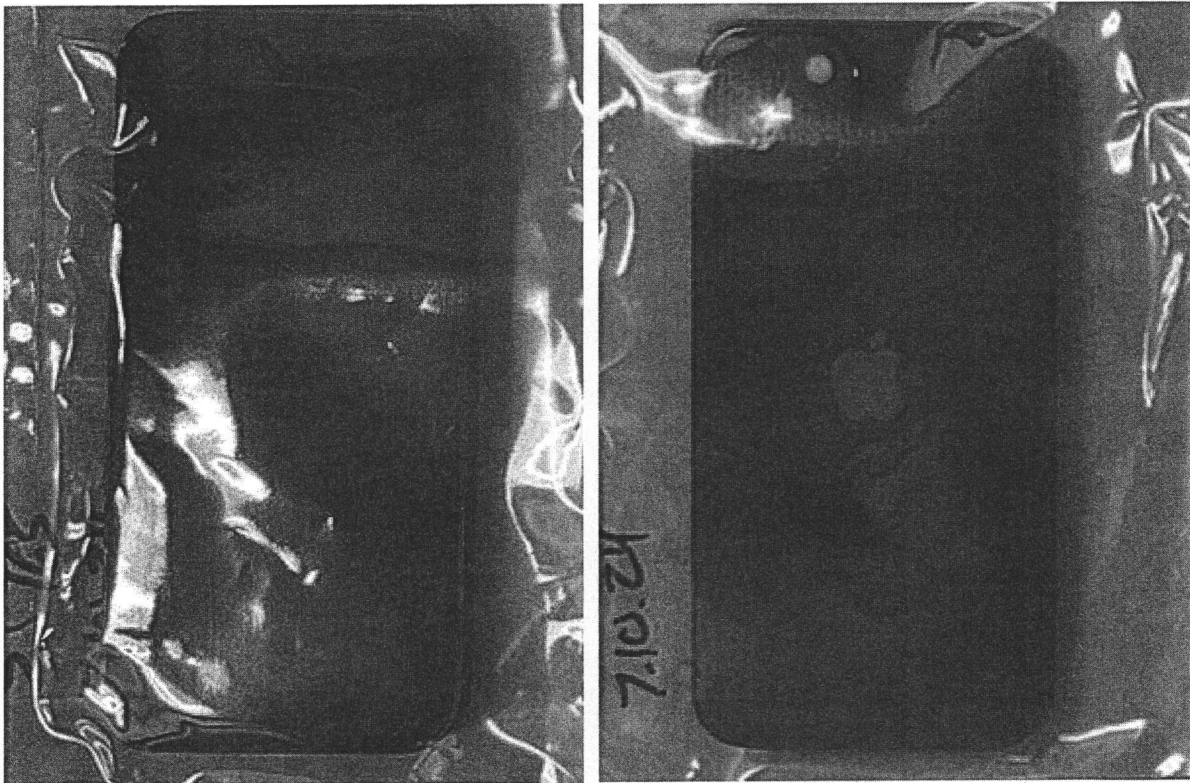
The property to be searched is a dark grey Apple iPhone that was initially seized by Gainesville Police Department on June 25, 2024, before being transferred to Homeland Security Investigations on January 31, 2025, as it was determined to be evidence in the criminal matter, including any Subscriber Identity Module (SIM) cards or other removable storage media contained therein. The front side of the Subject Telephone has a touch-screen display, and a camera is located near the middle of the top edge. The rear side of the Subject Telephone has three cameras in the top-left corner, and a metallic Apple logo is depicted near the middle. The Subject Telephone is currently stored at the Homeland Security Investigations office located at 1701 S. Columbus Hwy. Deming, NM 88030. The Subject Telephone is depicted below.



ATTACHMENT A3

PROPERTY TO BE SEARCHED

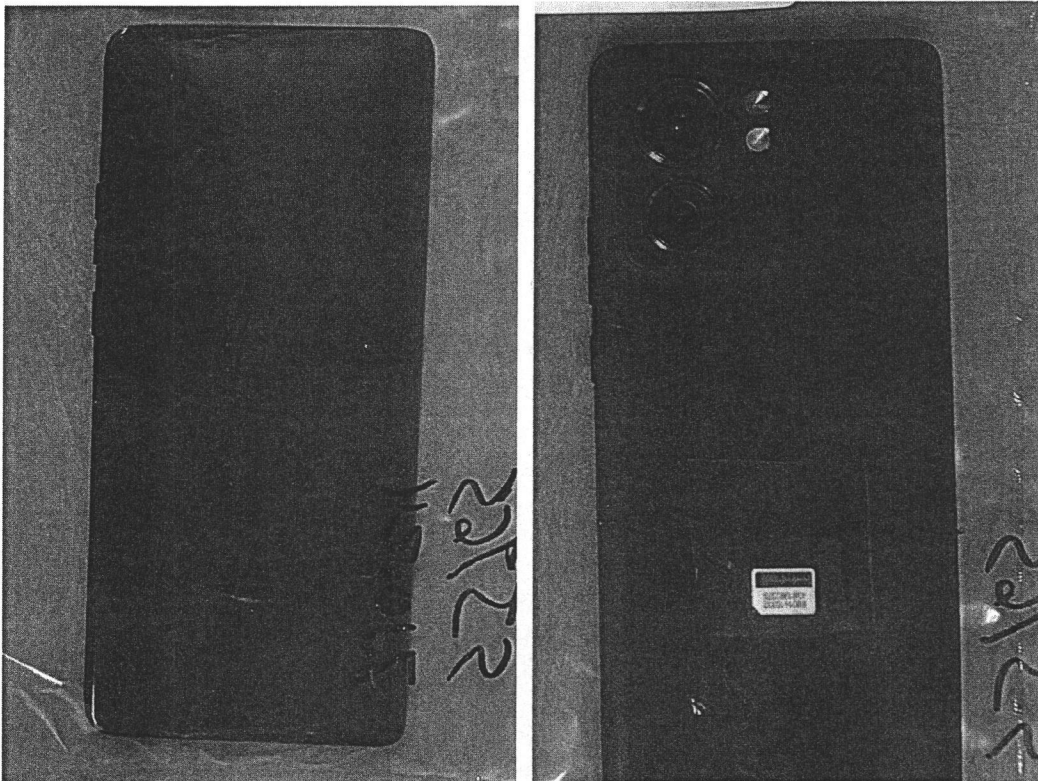
The property to be searched is a black Apple iPhone that was initially seized by Gainesville Police Department on June 25, 2024, before being transferred to Homeland Security Investigations on January 31, 2025, as it was determined to be evidence in the criminal matter, including any Subscriber Identity Module (SIM) cards or other removable storage media contained therein. The front side of the Subject Telephone has a touch-screen display, and a camera is located near the middle of the top edge. The rear side of the Subject Telephone has two cameras in the top-left corner, and a metallic Apple logo is depicted near the middle. The Subject Telephone is currently stored at the Homeland Security Investigations office located at 1701 S. Columbus Hwy. Deming, NM 88030. The Subject Telephone is depicted below.



ATTACHMENT A4

PROPERTY TO BE SEARCHED

The property to be searched is a black Motorola cell phone that was initially seized by Gainesville Police Department on June 25, 2024, before being transferred to Homeland Security Investigations on January 31, 2025, as it was determined to be evidence in the criminal matter, including any Subscriber Identity Module (SIM) cards or other removable storage media contained therein. The front side of the Subject Telephone has a touch-screen display. The rear side of the Subject Telephone has two cameras in the top-left corner, and a metallic Motorola logo is depicted near the middle. The Subject Telephone is currently stored at the Homeland Security Investigations office located at 1701 S. Columbus Hwy. Deming, NM 88030. The Subject Telephone is depicted below.



ATTACHMENT B

PARTICULAR THINGS TO BE SEIZED / INFORMATION TO BE RETRIEVED

The particular things to be seized include all records, wherever located and in whatever format, stored on the Subject Telephones described in Attachments A1, A2, A3, and A4 that are related to violations of 18 U.S.C. § 1956, and 18 U.S.C. § 1343, by Claudiu PESTELEU including:

1. Phone numbers, names, usernames, email addresses, residential addresses, and other identifying information of co-conspirators and other associates of the user of the Subject Telephones;
2. Audio and video calls made to or from the Subject Telephones, along with the duration and date and time each such communication occurred;
3. Any message logs or messages, whether sent from, to, or drafted on, the Subject Telephones, along with the date and time each such communication occurred;
4. The content of voice mail messages stored on the Subject Telephones, along with the date and time each such communication occurred;
5. Photographs or video recordings, along with the date and time each such photograph or video recording was created;
6. Information relating to the schedule, whereabouts, or travel of the user of the Subject Telephones;
7. Information relating to other methods of communications, including the contents of those communications, utilized by the user of the Subject Telephones stored on the Subject Telephones;
8. Bank records, checks, credit card bills, account information and other financial records;
9. Evidence of user attribution showing who used or owned the Subject Telephones, such

as social media accounts, email addresses, messages, location information, photographs and videos, phonebooks, saved usernames and passwords, documents, and internet browsing history.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, HSI shall deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

ATTACHMENT C

AFFIDAVIT IN SUPPORT OF ORDER AUTHORIZING SEARCH WARRANT

I, Juan C. Sanchez, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for search warrants authorizing the examination of the four cellphones described in Attachments A1, A2, A3 and A4, which are currently in law enforcement possession, and the extractions from the cellphones of the electronically stored information described in Attachment B.

AGENT BACKGROUND

2. I am a Special Agent with Homeland Security Investigations (HSI) and have been so employed since September 2021. I am currently assigned to HSI's Deming, New Mexico office. My primary responsibilities include investigating criminal violations of the United States Code in the district of New Mexico. My experience in this position has included but is not limited to interviewing suspects, witnesses, and victims; executing arrests and searches; collecting and processing evidence; analyzing records and digital evidence; and completing hundreds of hours of training in these topics and others, such as criminal law and financial crimes. I have also participated in numerous financial investigations involving HSI and other federal law enforcement agencies.

3. I am familiar with the facts and circumstances of this investigation because of my personal participation in the investigation, discussions with other agents involved in the

investigation, and review of reports written by other agents and other evidence and materials concerning the investigation.

4. Through my training and experience, I know that fraudsters often maintain one or more cellular or smart telephones (devices) which they use to further their fraud schemes. Fraudsters use these devices to facilitate logging on to, and communicating with representatives of, banking institutions and crypto currency exchanges, to communicate with fraud victims, and to communicate operational directives and information concerning the conduct of the organization's illegal activities to other members of the organization. I know based upon my training and experience that timely communication of financial information, such as bank account numbers, bank routing numbers, and virtual currency wallet identifiers, between organizational members and financial institutions, is critical to the overall success of the fraudster's illegal activities. The critical nature of this information is derived from the necessity of the organization's members to provide instructions for the receipt of monies from victims and subsequent transfer thereof to bank accounts and virtual currency wallets under their control.

5. I also know that some devices utilize subscriber identity module ("SIM") cards. A SIM card is a chip that is used to authenticate a device to a network. The SIM card generally contains subscriber information and authentication information, and it may contain contacts and encryption information. The portability of SIM cards in some devices allows a user to easily change devices, while maintaining the same telephone number, by removing the card from one device and inserting it into another. While SIM cards may have the capability to store some of the evidence described above, the storage capacity of devices tends to far exceed that of SIM cards. Which information is stored on the SIM card, on the device, or in both locations varies and depends on variables such as the user-defined settings on the device and the memory capacity of

the SIM card. Accordingly, information pertaining to fraud activity may be located on the SIM card itself, as well as the device in which the SIM card was inserted.

I further know from my training and experience that a cache of information concerning fraud activities such as bank account access, wire transfers, crypto currency exchange logins, crypto currency transfers, victim communications, bank and crypto currency exchange communications, and revealing the identity of the user of the device can be found on these devices. This information includes dialed, received, or missed calls and messages sent, received, or placed in draft status, which can be found on these devices, including in third-party applications (or “apps”) with messaging and audio and video calling features, such as Facebook Messenger, WhatsApp, SnapChat. I know that the identities, telephone numbers, and usernames of other participants involved in the fraud activity are often maintained in the contact lists of these devices, including in third-party social media and other applications. In my experience, fraudsters also use these devices to take and store photographs of themselves that they use to verify their identity for continued, unrestricted access to crypto currency exchanges. Fraudsters may also use GPS applications (such as Google Maps or Apple Maps), which can reveal their whereabouts when they conducted or arranged money withdrawals at banking institutions, activities or travel, as well as establishing identity of the user of the device based on the locations frequented. In my experience, the devices used by fraudsters are likely to contain evidence relating to their fraudulent activities including, but not limited to, contact lists, lists of recent call activity, stored text, chat, and voice mail messages, photographs and video recordings, GPS and location information, and financial accounts and records.

BACKGROUND CONCERNING VIRTUAL CURRENCY

6. **Virtual Currency:** Virtual currencies are digital representations of value that, like traditional coin and paper currency, function as a medium of exchange (i.e., they can be digitally traded or transferred, and can be used for payment or investment purposes). Virtual currencies are a type of digital asset separate and distinct from digital representations of traditional currencies, securities, and other traditional financial assets. The exchange value of a particular virtual currency generally is based on agreement or trust among its community of users. Some virtual currencies have equivalent values in real currency or can act as a substitute for real currency, while others are specific to particular virtual domains (e.g., online gaming communities) and generally cannot be exchanged for real currency. Cryptocurrencies, like Bitcoin and Ether, are types of virtual currencies, which rely on cryptography for security. Cryptocurrencies typically lack a central administrator to issue the currency and maintain payment ledgers. Instead, cryptocurrencies use algorithms, a distributed ledger known as a blockchain, and a network of peer-to-peer users to maintain an accurate system of payments and receipts.

7. **Virtual Currency Exchange:** A virtual currency exchange (VCE), also called a cryptocurrency exchange, is a platform used to buy and sell virtual currencies. VCEs allow users to exchange their virtual currency for other virtual currencies or fiat currency, and vice versa. Many VCEs also store their customers' virtual currency addresses in hosted wallets. For non-custodial instant VCEs, users do not create accounts nor are their funds held for any significant amount of time. VCEs can be centralized (i.e., an entity or organization that facilitates virtual currency trading between parties on a large scale and often resembles traditional asset exchanges like the exchange of stocks) or decentralized (i.e., a peer-to-peer marketplace where transactions occur directly between parties). To the extent they are operating wholly or in substantial part in

the U.S., VCEs may qualify as money services businesses (MSBs) under the Bank Secrecy Act. MSBs are legally required to conduct due diligence of their customers (i.e., know your customer checks to collect identifying information about customers and verify their identities) and to have anti-money laundering programs in place to the extent they operate and service customers in the United States or other countries with similar requirements. See 31 U.S.C. § 5311 et seq. (Bank Secrecy Act).

8. **Bitcoin:** Bitcoin (or BTC) is a type of virtual currency. Unlike traditional, government-controlled currencies (i.e., fiat currencies), such as the U.S. dollar, Bitcoin is not managed or distributed by a centralized bank or entity. Because of that, Bitcoin can be traded without the need for intermediaries. Bitcoin transactions are approved/verified by computers running Bitcoin's software. Those computers are called full nodes. Each node uses cryptography to record every Bitcoin transaction on the Bitcoin blockchain. The Bitcoin blockchain is a public, distributed ledger. Bitcoin can be exchanged for fiat currency, other virtual currencies, products, and services.

9. **Blockchain:** A blockchain is a digital ledger run by a decentralized network of computers referred to as "nodes." Each node runs software that maintains an immutable and historical record of every transaction utilizing that blockchain's technology. Many digital assets, including virtual currencies, publicly record all of their transactions on a blockchain, including all of the known balances for each virtual currency address on the blockchain. Blockchains consist of blocks of cryptographically signed transactions, and blocks are added to the previous block after validation and after undergoing a consensus decision to expose and resist tampering or manipulation of the data. There are many different blockchains used by many different virtual

currencies. For example, Bitcoin in its native state exists of the Bitcoin blockchain, while Ether (or ETH) exists in its native state on the Ethereum network.

10. **Blockchain Analysis:** Law enforcement can trace transactions on blockchains to determine which virtual currency addresses are sending and receiving particular virtual currency. This analysis can be invaluable to criminal investigations for many reasons, including that it may enable law enforcement to uncover transactions involving illicit funds and to identify the person(s) behind those transactions. To conduct blockchain analysis, law enforcement uses reputable, free open-source blockchain explorers, as well as commercial tools and services. These commercial tools are offered by different blockchain-analysis companies. Through numerous unrelated investigations, law enforcement has found the information associated with these tools to be reliable. The third-party blockchain-analysis software utilized in this case is an anti-money laundering software provided by Company A. This software is used by financial institutions and law enforcement organizations worldwide. This third-party blockchain analysis software has supported many investigations and has been referenced in numerous search and seizure warrants, and as such, has been found to be reliable. Law enforcement has been able to verify the reliability of this software by ex-post analysis. For example, in an unrelated case where the government used Company A's clustering software, the government's blockchain analysis identified over 50 customers of a darknet child pornography site. In each one of the 50 subsequent law enforcement actions, the blockchain analysis was corroborated by statements and search warrant returns from the targets' devices. In sum, this software has correctly analyzed

data on the blockchain in hundreds of investigations, and I have assisted or been briefed on many of these investigations.

11. **Virtual Currency Wallet:** A virtual currency wallet (e.g., a hardware wallet, software wallet, or paper wallet) stores a user's public and private keys, allowing a user to send and receive virtual currency stored on the blockchain. Multiple virtual currency addresses can be controlled by one wallet.

- a. **Hardware Wallet:** A hardware wallet is a physical, removable device that stores a user's private keys and can be connected to a computer when a user wishes to use the keys stored on the wallet for virtual currency transactions. Hardware wallets can be secured with PINs and passphrases and can be backed up or regenerated with a recovery phrase. Trezor and Ledger are some examples of the types of hardware wallets on the market.
- b. **Hosted Wallet:** A hosted wallet, also known as a custodial wallet, is a virtual currency wallet through which a third party, e.g., a virtual currency exchange, holds a user's private keys. The third party maintains the hosted wallet on its platform akin to how a bank maintains a bank account for a customer, allowing the customer to authorize virtual currency transactions involving the hosted wallet only by logging into/engaging with the third party's platform.
- c. **Paper Wallet:** A paper wallet is an offline paper record of a virtual currency wallet's public and private keys. Paper wallets can include barcodes (e.g., a QR

code) along with their alphanumeric strings. It is literally private keys printed on a piece of paper.

- d. **Software Wallet:** A software wallet is an internet-connected virtual currency wallet in the form of a software application on a desktop or mobile device or a web-based platform accessible through a web browser. The software will store and usually encrypt the user's public and private keys.
- e. **Unhosted Wallet:** An unhosted wallet, also known as a self-hosted or non-custodial wallet, is a virtual currency wallet through which the user has complete control over storing and securing their private keys and virtual currency. Unhosted wallets do not require a third party's involvement (e.g., a virtual currency exchange) to facilitate a transaction involving the wallet.

12. **Darknet Markets:** "Darknet markets" are commercial websites that are typically hosted as Tor onion services. Darknet markets primarily function as black markets where one can sell or broker transactions involving illegal drugs, cybercriminal tools (e.g., malware), weapons, counterfeit currency, stolen personally identifiable information, forged documents and identification credentials, and other illicit goods and services. BTC is the most common method of payment for products and services procured on darknet markets.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

13. The property to be searched is one Grey Apple iPhone, one Dark Grey Apple iPhone, one Black Apple iPhone and one Black Motorola cell phone, and any SIM card or other storage media contained therein, hereinafter "the Subject Telephones." The Subject Telephones were retrieved from Claudiu PESTELEU on June 25, 2024. The Subject Telephones are currently located at the Homeland Security Investigations office located at 1701 S. Columbus Highway

Deming, NM 88030. In my training and experience, I know that the Subject Telephones have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Subject Telephones came into the possession of HSI on January 31, 2025. We understand that the Subject Telephones were searched by Gainesville Police Department (GPD) pursuant to a search warrant issued by the Circuit Court of the Eight Judicial Circuit in and For Alachua County, Florida, but to date we have not received the results of the search.

14. The applied-for warrants would authorize the forensic examination of the Subject Telephones for the purpose of identifying electronically stored data particularly described in Attachment B.

BACKGROUND CONCERNING THE INVESTIGATION

15. In August of 2023, HSI Deming began investigating a large-scale criminal conspiracy involving CLAUDIU PESTELEU, and other known and unknown persons, for committing violations of and relating to 18 U.S.C. § 1956 and 18 U.S.C. § 1343. CLAUDIU PESTELEU is believed to have the following aliases: Matthias Zammer; Thomas Muller; Samuel Der Saar; Boris Adler, Fritz Bittman and Fred Laport.

16. In furtherance of the conspiracy, the subjects under investigation create and/or cause to be created web pages and/or sites falsely purporting to be legitimate businesses advertising vehicles, boats, farm equipment, heavy machinery, and other conveyances available for sale and/or auction online.

17. Many pages and/or sites are designed to strongly resemble those of actual legitimate dealerships, often including high resolution photographs, video showcases, and virtual tours that conspirators duplicate from legitimate dealerships' websites. In some instances, the websites have

additional sophisticated features such as chat bots that enable customers to communicate with representatives of the “seller” in real-time.

18. In fact, the “sellers” represented by the co-conspirators to be legitimate businesses were either (1) an entirely fictitious business that has no legitimate incorporation filings or physical location, or (2) a current or formerly legitimate business that was previously incorporated and has / had a physical location, digital footprint, et cetera.

19. The conspirators regularly create and/or cause to be created numerous web pages and sites corroborating the existence of the fraudulent “seller.” Examples include postings to various commercial car sales websites such as Kelly Blue Book, CarFax, AutoTrader, Cars.com et cetera, as well as postings to social media web sites, such as Facebook, and various consumer directories and mapping services such as Google Maps.

20. After being contacted by victims who locate the advertisements and express interest in completing purchases, the conspirators routinely communicate with victims by way of electronic mail, text messaging, chat messaging, and/or telephone. In doing so, conspirators often negotiate regarding the purchase price and/or delivery fees; offer to schedule appointments during which victims can inspect the item in person; and send additional documentation corroborating the existence of the purported seller and product, including photos and videos not included in the original advertisement; fraudulent history and service reports; warranties; refund policies and money-back guarantees; et cetera. If fraudulently misrepresenting themselves as staff from a legitimate dealership, conspirators also often send copies of the legitimate organization’s historical incorporation records and/or business licenses, which are obtainable through the appropriate regulatory agencies.

21. After victims agree to complete the purchase for a negotiated price and delivery

fee, conspirators provide the victims and/or their banking representatives with wiring instructions and fraudulent titles, bills of sale, purchase orders, and/or invoices. The conspirators further advise victims that they will initiate delivery after the funds transfer is complete.

22. The actions outlined in the preceding paragraphs serve to legitimize the conspirators' fraudulent activities and dispel any potential suspicions from victims, bank officials reviewing loan applications and/or wire transfer requests, and law enforcement with whom victims inquire about the legitimacy of the "seller." In effect, this maximizes the probability that potential victims will ultimately transfer funds to the conspirators to complete purchases.

23. After receiving victims' funds, conspirators ultimately terminate contact with the victims and fail to deliver the purchased product. The bank accounts into which conspirator(s) direct victims to transfer funds are held by beneficiary entities that, while officially incorporated, are otherwise illegitimate shell companies. Unlike many of the purported "seller" entities, these corporations are exclusively controlled by conspirators and lack any association to existing or formerly legitimate companies. Using aliases and fraudulent identification documents purportedly issued by foreign nations, the conspirators establish these entities and bank accounts to receive, layer, and/or launder fraud proceeds.

RELEVANT TARGET ENTITIES

24. According to records from Florida Department of State, Division of Corporations, Zammer Equipment LLC ("Zammer Equipment") is a Florida-registered Limited Liability Company organized on May 26, 2023, principal office located in Jacksonville, FL, whose authorized member is "Matthias Zammer." "Matthias Zammer" is a known alias of CLAUDIU PESTELEU.

25. Super Exotic Deals LLC ("Super Exotic Deals") is a Florida-registered Limited

Liability Company organized on March 07, 2024, principal office located in Pembroke Pines, FL, whose authorized member is “Samuel Der Saar.” “Samuel Der Saar” is an alias of CLAUDIU PESTELEU.

26. Equipment Types Machinery LLC (“Equipment Types Machinery”) is a Florida-registered Limited Liability Company organized on July 28, 2023, principal office located in Jacksonville, FL, whose authorized member is “Dino Gustavson.” “Dino Gustavson” is believed to be an alias of Co-Conspirator 2.

27. Adler Pre Owned LLC (“Adler Pre Owned”) is a Florida-registered Limited Liability Company organized on July 25, 2023, principal office located in Palmetto Bay, FL, whose authorized member is “Boris Adler,” who is believed to be an alias for Claudiu PESTELEU.

28. Bittman Motors LLC (“Bittman Motors”) is a Florida-registered Limited Liability Company organized on June 01, 2023, principal office located in Jacksonville, FL, whose authorized member is “Fritz Bittman,” who is believed to be an alias for an Claudiu PESTELEU.

RELEVANT TARGET BANK ACCOUNTS

29. JPMorgan Chase Bank, N.A. account ending in “1672” associated with “Boris Adler,” who is believed to be an alias for Claudiu PESTELEU.

30. Bank of America, N.A. account ending in “2238” titled to “Matthias Zammer” opened on June 06, 2023, by “Matthias Zammer,” which is a known alias of CLAUDIU PESTELEU, in Jacksonville, FL.

31. Bank of America, N.A. account ending in “8038” titled to Zammer Equipment opened on June 06, 2023, by managing member “Matthias Zammer,” which is a known alias of CLAUDIU PESTELEU, in Jacksonville, FL.

32. Truist bank account ending in “7893” is associated with “Fred Laport” by way of

surveillance footage and another record from a branch located in Miami Beach, FL, dated June 04, 2024, depicting CLAUDIU PESTELEU, withdrawing \$12,000.00 in United States currency.

33. Truist bank account ending in "0869" is associated with "Samuel Der Saar," and Super Exotic Deals, by way of surveillance footage and another record from a branch located in Dallas, TX, dated June 20, 2024, depicting CLAUDIU PESTELEU, withdrawing \$15,000.00 in United States currency.

34. SouthState Bank, N.A. account ending in "8804" is associated with "Fritz Bittman," who is believed to be an alias for Claudiu PESTELEU.

PROBABLE CAUSE

35. Because this Affidavit is being submitted for the limited purpose of establishing probable cause, I have not included each and every known fact regarding the investigation. More specifically, I have set forth only pertinent facts that I believe are necessary to establish probable cause to search the Subject Telephones for evidence of violations of 18 U.S.C. § 1349 and 18 U.S.C. § 1956(h).

36. The request to search the Subject Telephones is based on the following:

37. CLAUDIU PESTELEU is associated with the Super Exotic Deals Bank of America, N.A. account ending in "6533," by way of one suspected fraudulent or counterfeit Belgium Passport, in the name of "Samuel Der Saar," that he was in possession of during an arrest on or about June 25, 2024, by GPD. The photograph on the suspected fraudulent or counterfeit Belgium passport appears to be CLAUDIU PESTELEU with medium-to-long facial hair.

38. On or about September 11, 2024, HSI Deming received supporting documentation from Bank of America, N.A. for Super Exotic Deals' account ending in "6533." A review of the supporting documentation revealed that on April 10, 2024, there was a \$215,000.00 wire transfer

credit posted to Super Exotic Deals' Bank of America, N.A. account ending in "6533," and at least one cash withdrawal, in the sum of \$20,000.00, whose description indicates it occurred in Sunny Isles Beach, FL. Supporting documentation also revealed the address associated with Super Exotic Deals was in Pembroke Pines FL.

39. In September of 2024, a previously identified victim, who is from Greenville, Michigan, informed HSI Deming that the previously identified victim was defrauded of \$22,200.00, by Adler Pre Owned, after the previously identified victim transmitted one wire transfer for one Caterpillar skid steer that the previously identified victim never received.

40. In or about December of 2023, a previously identified victim communicated with unknown person(s), via electronic mail, whom the previously identified victim believed were representatives of an impersonated business, regarding the purchase of one Caterpillar skid steer that the previously identified victim saw for sale on an impersonated business website.

41. The previously identified victim was provided an invoice that read, in part: "[Impersonated Business]" and contained wiring instructions that read, in part: "Business Account Name: ADLER PRE OWNED, LLC."

42. On or about December 27, 2023, the previously identified victim wire transferred \$22,200.00, to "Boris Adler," who is believed to be an alias for Claudiu PESTELEU, JPMorgan Chase Bank, N.A. account ending in "1672" to affect the purchase of one Caterpillar skid steer.

43. In November of 2024, HSI Deming obtained records from Kraken, which is a virtual currency exchange, concerning account #: AA28 N84G QKE3 XDDA created on May 30, 2023, associated with the name "Fritz Bittman" and user identification "fritz511." Kraken account #: AA28 N84G QKE3 XDDA is associated with SouthState Bank account ending in 8804 by way of one deposit on August 09, 2023. A previously identified fraud victim wired

\$42,900.00, to SouthState Bank account ending in 8804, on or about September 13, 2023, to affect the purchase of one 2015 Airstream.

44. Kraken account #: AA28 N84G QKE3 XDDA opening and verification documents include a photo of what appears to be Austrian passport #: U117335, which bears the name Fritz Bittman; the date of birth July 15, 1990; and a photograph of a male who appears to be Claudiu PESTELEU. The passport further indicates that it was issued in Braunau, Austria on October 31, 2020. All account opening and verification documents appear to be photographs taken by an electronic device such as a cellular phone.

45. In November of 2024, HSI Deming obtained records from Kraken, which is a virtual currency exchange, concerning account #: AA51 N84G D3O7 SSAA created on September 13, 2023, associated with the name "Boris Adler" and user identification "borisadler7." On November 29, 2023, "borisadler7" electronically corresponded with Kraken customer support and wrote, in part:

46. *"Fuck You all mother fuckers. I will report you for laundering money. I know a lot of things and I have proof. It will be nationwide news because I can prove 5 millions of dollars being sent by me to you within a year! Mother fuckers!"*

47. Kraken account #: AA51 N84G D3O7 SSAA opening and verification documents include photo of what appears to be Deutschland passport #: CFL0N2K75, which bears the name Boris Adler; the date of birth October 31, 1991; and a photograph of a male who appears to be Claudiu PESTELEU. The passport further indicates that it was issued under Stadt Wolfsburg authority on February 01, 2020. All account opening and verification documents appear to be photographs taken by an electronic device such as a cellular phone.

48. In September of 2024, a previously identified victim, who is from Phoenix, Arizona

informed HSI Deming that the previously identified victim was defrauded of \$42,900.00, by Bittman Motors, after the previously identified victim transmitted one wire transfer for one 2015 Airstream that the previously identified victim never received.

49. In or about September of 2023, the previously identified victim communicated with unknown person(s), telephonically and via electronic mail, who the previously identified victim believed were representatives of an impersonated business, regarding the purchase of one 2015 Airstream that the previously identified victim saw for sale on a Google Sites web page purporting to be associated with the impersonated business.

50. On or about September 13, 2023, the previously identified victim wire transferred \$42,900.00, to Bittman Motors, which is associated with "Fritz Bittman", who is believed to be an alias for Claudiu PESTELEU, SouthState Bank, N.A. account ending in "8804" to affect the purchase of one 2015 Airstream.

51. On June 25, 2024, GPD conducted a traffic stop on a grey BMW X7 and arrested a passenger who identified himself as "Thomas Muller," a known alias of CLAUDIU PESTELEU, and provided "Deutschland" identification in that name, for numerous state offenses related to narcotics and fraudulent document possession. During CLAUDIU PESTELEU's arrest, GPD seized multiple devices and suspected fraudulent documents from CLAUDIU PESTELEU, including but not limited to:

- a. Grey Apple iPhone (PESTELEU's – located on the rear passenger's seat)
- b. Dark Grey Apple iPhone (PESTELEU's – located on his person)
- c. Black Apple iPhone (PESTELEU's – located in his toiletry bag on the rear passenger's seat)
- d. Black Motorola cell phone (PESTELEU's – located in his toiletry bag on the rear

passenger's seat)

- e. One Belgium passport, number ending in "3617" in the name of "Samuel Der Saar," with male photograph depicting who appears to be CLAUDIU PESTELEU.
- f. One JPMorgan Chase Bank N.A. card ending in "4101" in the name of "Samuel Der Saar".
- g. One Wells Fargo Bank card ending in "8406" in the name of "Samuel Der Saar".
- h. One Wells Fargo bank card ending in "7738" in the names of "Samuel Der Saar" and Super Exotic LLC.
- i. One Luxembourg passport, number ending in "0307" in the name of "Fred Laport," with male photograph depicting who appears to be CLAUDIU PESTELEU.

52. Following CLAUDIU PESTELEU's arrest, ICE Enforcement and Removal Operations (ERO) compared "Thomas Muller's" fingerprints against those collected from CLAUDIU PESTELEU during previous primary inspections upon entering the United States. The fingerprints matched, thereby identifying "Thomas Muller" as CLAUDIU PESTELEU.

53. In July of 2024, HSI Special Agents interviewed "Thomas Muller" at the Alachua County Jail in Gainesville, Florida. When asked what he would like to be called during the interview, "Thomas Muller" identified himself as CLAUDIU PESTELEU and stated that he was born in Debrecen, Hungary in October of 1981.

54. On July 12, 2024, HSI Deming received information indicating that on July 9, 2023, the St. Johns County, Florida Sheriff's Office (SJCSO) stopped a white 2023 BMW X7. During the stop, SJCSO Deputies encountered two male subjects who identified themselves as "Thomas Muller" and the person believed to be Co-Conspirator 2.

55. CLAUDIU PESTELEU appeared to be one and the same as the person depicted in

surveillance records withdrawing cash from Zammer Equipment Bank of America, N.A. account ending in “8038,” and “Matthias Zammer,” which is a known alias of CLAUDIU PESTELEU, who is associated with Bank of America, N.A. account ending in “2238,” as well as the person depicted in Belgium passport in the name of “Samuel Der Saar.”

56. CLAUDIU PESTELEU appeared to be one and the same as the person depicted in surveillance records withdrawing cash on June 04, 2024, “Fred Laport,” which is a known alias of CLAUDIU PESTELEU, Truist bank account ending in “7893,” as well as the person depicted in Luxembourg passport in the name of “Fred Laport.” The withdrawn cash is believed to be proceeds from victims.

57. CLAUDIU PESTELEU appeared to be one and the same as the person depicted in surveillance records withdrawing cash on June 20, 2024, from Super Exotic Deals Truist bank account ending in “0869,” associated with “Samuel Der Saar,” which is a known alias of CLAUDIU PESTELEU. The withdrawn cash is believed to be proceeds from victims.

58. To date, HSI Deming has identified at least fifteen victims who collectively transferred approximately \$525,000, to accounts controlled by Zammer Equipment, as well as two victims who collectively transferred \$327,000 to bank accounts controlled by “Samuel Der Saar”, and/or Super Exotic Deals, prior to CLAUDIU PESTELEU’s arrest.

59. Based on my training, experience, and research, I know that devices, such as the Subject Telephones, possess capabilities that allow them to serve as a wireless telephone, digital camera, and GPS navigation device. Additionally, the Subject Telephones have both web browsing and Wi-Fi capabilities. In my training and experience, examining data, including location data, stored on devices of this type can uncover, among other things, evidence that reveals or suggests

who possessed or used the devices as well as when the individual used the device and where they were when they used the devices.

60. Based upon the information contained in this Affidavit, there is probable cause to believe that the Subject Telephones contain evidence of violations of 18 U.S.C. § 1349: conspiracy to commit wire fraud, and 18 U.S.C. § 1956(h): conspiring to launder monetary instruments.

ELECTRONIC STORAGE & FORENSIC ANALYSIS

61. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. This information can sometimes be recovered with forensics tools.

62. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Subject Telephones were used, the purpose of their use, who used the Subject Telephones, and when. There is probable cause to believe that this forensic electronic evidence might be on the Subject Telephones because:

- a. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- b. A person with appropriate familiarity with how an electronic device works and the data generated by such devices may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

- c. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- d. Further, in finding evidence of how devices were used, the purpose of their use, who used them, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

63. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Subject Telephones consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Subject Telephones to human inspection in order to determine whether it is evidence described by the warrant.

64. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

65. Based on the above information, there is probable cause to believe that evidence of violations of 18 U.S.C. § 1349 and 18 U.S.C. § 1956(h) are in the Subject Telephones. Therefore,

I respectfully request that this Court issue a search warrant for the Subject Telephones, more particularly described Attachments A1, A2, A3, and A4 authorizing the seizure and examination of the items described in Attachment B.

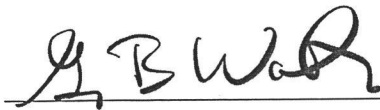
Respectfully Submitted,



Juan Sanchez
Special Agent
Homeland Security Investigations

Electronically submitted and telephonically

sworn to before me on February 27, 2025



The Honorable **Gregory B. Wormuth**
United States Magistrate Judge